JP11234264

WPI

TI - Electronic watermark system for electronic information distributing system - multiplies random number in portion of encryption lock and enables user to choose one of encryption keys, corresponding to encryption informations, and transmitted encryption information

AB - JP11234264 NOVELTY - A random number is multiplied in a portion of an encryption lock. A user chooses one of the encryption keys, corresponding to encryption informations, and a transmitted encryption information. The encryption keys and the encryption informations are transmitted to the user by a server. DETAILED DESCRIPTION - The encryption key is generated by performing the encryption of a predetermined encryption key using another predetermined encryption key. The encryption information is generated by performing the encryption of for every generated information using the predetermined encryption key. INDEPENDENT CLAIMS are also included for the following:an electronic information distributing system; and a memory medium.

- USE - For electronic information distributing system. Used for protecting copyright of digital information, e.g. moving image data, still picture image data, audio data, computer data, computer program, which is distributed in a multimedia network.

- ADVANTAGE - Prevents making a reverse process of the encryption key and a random number. Prevents a server from embedding user information freely and distributing the user information unjustly. Increases the operating efficiency of the electronic watermark system. Prevents inaccurate distribution of digital data. DESCRIPTION OF DRAWING(S) - The figure shows a diagram explaining an implanting process.
- (Dwg.1/8)

PN - JP11234264 A 19990827 DW199945 H04L9/36 015pp
PR - JP19980034770 19980217
PA - (CANO) CANON KK
MC - T01-H01C2 T03-P01 W01-A05 W02-J03A2B W03-A W04-F
DC - P85 T01 T03 W01 W02 W03 W04
IC - G06F12/14 ;G09C5/00 ;G11B20/10 ;H04L9/36 ;H04N1/387 ;H04N5/91 ;H04N7/08 ;H04N7/081
AN - 1999-535482 [45]

Random number as w/m?
Nothing about removal / invisible.
Not perceptible?

PAJ

TI - ELECTRONIC PAPERMARKING SYSTEM, ELECTRONIC INFORMATION DISTRIBUTION SYSTEM USING THE SAME AND STORAGE MEDIUM

AB - PROBLEM TO BE SOLVED: To surely prevent an illegal use of digital data and to decrease the amount of communication or calculation to be performed for preventing the illegal use.

- SOLUTION: This is an electronic papermarking system wherein a server performs a first processing for generating plural pieces of different electronic papermark information, a second processing for generating plural pieces of enciphered information by enciphering these plural pieces of information while using individual cryptographic keys for each piece, a third processing for generating plural enciphered cryptographic keys by enciphering these individual cryptographic keys by multiplying a random number and a fourth processing for transmitting the plural pieces of enciphered information and the plural enciphered cryptographic keys as mentioned above to a user, while a user performs a fifth processing for selecting one of the plural pieces of transmitted enciphered information or one of the plural enciphered cryptographic keys corresponding to the enciphered information. A safe and highly efficient system concerning the illegal distribution of digital data can be provided by multiplying the random number only to the partial cryptographic key when multiplying the random number to the individual cryptographic keys.

PN - JP11234264 A 19990827
PD - 1999-08-27
ABD - 19991130
ABV - 199913
AP - JP19980034770 19980217
PA - CANON INC
IN - IWAMURA KEIICHI
I - H04L9/36 ;G06F12/14 ;G09C5/00 ;G11B20/10 ;H04N1/387 ;H04N5/91 ;H04N7/08 ;H04N7/081

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－234264

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		

審査請求　未請求　請求項の数22　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平10－34770

(22)出願日　平成10年(1998)２月17日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

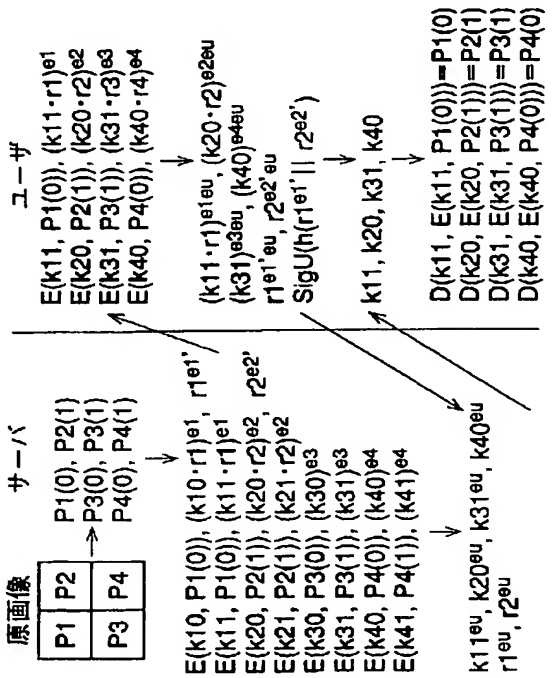
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　電子透かし方式及びそれを用いた電子情報配布システム並びに記憶媒体

(57)【要約】

【課題】　ディジタルデータが不正に使用されるのを確実に防止できるようにするとともに、不正使用を防止するために行う通信量や計算量を減少できるようにする。

【解決手段】　電子透かし情報の異なる複数の情報を生成する第１の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第２の処理と、上記個別の暗号鍵に乱数を乗じて暗号化して複数の暗号化暗号鍵を生成する第３の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第４の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の１つを選択する第５の処理を上記ユーザが行う電子透かし方式において、上記個別の暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数を乗じることにより、ディジタルデータの不正配布に関して安全で高効率なシステムを実現できるようにする。



【特許請求の範囲】
【請求項１】　電子透かし情報の異なる複数の情報を生成する第１の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第２の処理と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第３の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第４の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の１つを選択する第５の処理を上記ユーザが行う電子透かし方式において、
上記暗号鍵の一部にのみ乱数を乗じることを特徴とする電子透かし方式。
【請求項２】　上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信することを特徴とする請求項１に記載の電子透かし方式。
【請求項３】　上記電子透かしの正当性を検証する処理を行うことを特徴とする請求項１または２に記載の電子透かし方式。
【請求項４】　電子透かしの正当性を検証する処理を繰り返して行うことを特徴とする電子透かし方式。
【請求項５】　電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子透かし方式において、
上記ユーザの電子透かし情報を検査する処理を行うことを特徴とする電子透かし方式。
【請求項６】　上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する処理を行うことを特徴とする請求項１～５の何れか１項に記載の電子透かし方式。
【請求項７】　上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを用いることを特徴とする請求項１～６の何れか１項に記載の電子透かし方式。
【請求項８】　画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットであって、上記請求項１～６の何れか１項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを用いることを特徴とする請求項１～６の何れか１項に記載の電子透かし方式。
【請求項９】　請求項１～６の何れか１項に記載の電子透かし方式の手順をコンピュータに実行させるためのプログラムを格納したことを特徴とする記憶媒体。
【請求項１０】　上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを格納したことを特徴とする記憶媒体。
【請求項１１】　画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットを格納した記憶媒体において、
上記請求項１～５の何れか１項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを格納したことを特徴とする記憶媒体。
【請求項１２】　電子透かし情報の異なる複数の情報を生成する第１の手段と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第２の手段と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第３の手段と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第４の手段とをサーバが有し、上記送信された複数の暗号化情報や、上記暗号化情報に対応する暗号化暗号鍵の１つを選択する第５の手段をユーザが有する電子情報配付システムにおいて、
上記暗号鍵の一部にのみ乱数を乗じるようにする第６の手段をサーバに設けたことを特徴とする電子情報配付システム。
【請求項１３】　上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信する第７の手段を更に有することを特徴とする請求項１２に記載の電子情報配付システム。
【請求項１４】　上記電子透かしの正当性を検証する第８の手段をさらに有することを特徴とする請求項１２または１３に記載の電子情報配付システム。
【請求項１５】　電子透かしの正当性を検証する処理を繰り返し行うようにしたことを特徴とする電子情報配付システム。
【請求項１６】　電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子情報配付システムにおいて、
上記ユーザの電子透かし情報を検査する検査手段を有することを特徴とする電子情報配付システム。
【請求項１７】　上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する検査手段をさらに有することを特徴とする請求項１２～１６の何れか１項に記載の電子情報配付システム。
【請求項１８】　上記暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報をヘッダ部に有する画像フォーマットを用いることを特徴とする請求項１２～１６の何れか１項に記載の電子情報配付システム。
【請求項１９】　画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットであって、上記請求項１２～１６の何れか１項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを用いることを特徴とする請求項１２～１６の

何れか１項に記載の電子情報配付システム。
【請求項２０】　請求項１２～１６の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴とする記憶媒体。
【請求項２１】　上記暗号化手段により行われる暗号化処理及び／または電子透かし埋め込み手段により行われる電子透かし埋め込み処理を検査するための検査情報をヘッダ部に有する画像フォーマットを格納したことを特徴とする記憶媒体。
【請求項２２】　画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットを格納した記憶媒体において、
上記請求項１２～１６の何れか１項に記載の暗号化手段により行われる暗号化処理及び／または電子透かし埋め込み手段により行われる電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを格納したことを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は電子透かし方式及びそれを用いた電子情報配布システム並びに記憶媒体に関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のディジタル情報における著作権を保護するための電子透かし技術、及びそれを用いてディジタル情報の配布を行うマルチメディアネットワークに用いて好適なものである。
【０００２】
【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。上記ネットワーク上で取引される商品として、画像等を含むディジタルデータが考えられる。
【０００３】しかし、ディジタルデータは完全なコピーを容易に、かつ大量に作成できるという性質を有しているので、そのディジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配付することができるという可能性を持っている。ディジタルデータが不正に作成されて再配布されてしまうと、本来は著作者または著作者から正当に販売を委託された者（販売者）に支払われるべき代価が支払われず、著作権が侵害されてしまう恐れがある。
【０００４】一方、著作者または販売者（以後、ディジタルデータを正当に配布する者をサーバと呼ぶ）がディジタルデータを１度ユーザに送ってしまうと、上記の不正コピーを完全に防止することはできない。そこで、不正コピーを直接防止するのではなく、電子透かしと呼ばれ、著作権の保護に役立つ手法が提案されている。
【０００５】上記電子透かしとは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する著作権情報やユーザに関する利用者情報をディジタルデータ中に埋め込むことによって、不正コピーが見つかった場合にディジタルデータを誰が再配布したのかを特定するための手法である。
【０００６】電子透かしを用いる従来のシステムでは、サーバは完全に信頼できる機関であることが前提となっている。このため、サーバが信頼できる機関ではなく不正を行う可能性があるとすると、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう恐れがある。
【０００７】これは、従来の電子透かしを用いるシステムは、サーバがユーザを特定するために用いる利用者情報をディジタルデータ（以後、ディジタルデータを画像データとして説明する）に埋め込むので、サーバが勝手に利用者情報を埋め込みそのコピーを不正に配布した場合、その利用者情報から特定されるユーザは、サーバの主張を退ける手段がないためである。その対策として、いくつかの手法が提案されている。例えば、図４に示したような手法が提案されている。
【０００８】〔埋め込み処理〕図４に示した手法は、先ず、第１の埋め込み処理として、サーバは、原画像をＮ個のブロックに分割し、各ブロックをＰｎ（ｎ＝１，…，Ｎ）とおく。次に、各ブロックＰｎをＮｓ個（Ｎｓ＜Ｎ）のＳブロックと、Ｎｕ個（Ｎｕ＝Ｎ－Ｎｓ）のＵブロックとに分ける。
【０００９】図４では、原画像を４分割し、上側のブロックＰ１、Ｐ２をＳブロックとし、下側のブロックＰ３、Ｐ４をＵブロックとしている。また、サーバは暗号鍵ｋによってデータＰを暗号化する暗号化手段Ｅ（ｋ，Ｐ）を準備する。
【００１０】一方、ユーザは、それに対応する復号手段を持つ。また、サーバとユーザは独立に「ｅ・ｄ＝１　ｍｏｄ　ｐ－１」となる変数ｅとｄを生成する。ただし、ｐ＝２ｑ＋１〔ｑは素数〕であり、サーバは以上のような変数ｅとｄを２・Ｎ組生成し、（ｅｎ、ｄｎ）とおく（ユーザのｅとｄはｅｕ，ｄｕとおく）。
【００１１】次に、第２の埋め込み処理として、サーバは、Ｓブロックにユーザ毎に定めたユーザ情報を埋め込み、Ｕブロックの複製を2^b個生成して０～2^b－１の数値を埋め込む。以降、ブロックＰｎに数値ｉが埋め込まれた時それをＰｎ（ｉ）と表現する。
【００１２】図４では、ＳブロックであるＰ１、Ｐ２にユーザ情報として｛０，１｝が埋め込まれ、ｂ＝１としてＵブロックであるＰ３，Ｐ４の２個の複製に対して０と１の数値が埋め込まれている。
【００１３】次に、第３の埋め込み処理として、サーバは、ＳブロックのＰｎ（ｉ）の複製を2^b個生成し、各々異なる暗号鍵ｋｎｊ（ｊ＝０，…，2^b－１）で暗号化したＥ（ｋｎｊ，Ｐｎ（ｉ））と、暗号鍵ｋｎｊに乱数ｒｎをかけてｅｎで暗号化した$(knj \cdot rn)^{en}$を

ともにユーザに送る。さらに、$Nu \cdot 2^b$ 個のUブロックPn（i）を各々kniで暗号化したE（kni，Pn（j））と暗号鍵kniに乱数rnをかけてenで暗号化した（kni・rn）^{en}をともにユーザに送る。

【0014】また、サーバは乱数rnをen'（n'＝N＋n）で暗号化した暗号化乱数rn^{en}を保存し、かつユーザに送る。以後、暗号化手段E（k，P）によって暗号化した画像を暗号化画像、暗号鍵に乱数をかけてenで暗号化したものをサーバ暗号化暗号鍵、またen'で暗号化した乱数をサーバ暗号化乱数と呼ぶ。このとき、暗号化画像やサーバ暗号化暗号鍵、サーバ暗号化乱数はその対応が正しければランダムに送ることができる。

【0015】次に、第4の埋め込み処理として、ユーザは、送られてきた複数の暗号化画像とサーバ暗号化暗号鍵のペアの中から各ブロック毎に1つづつのペアを選ぶ。図4では、各ブロック毎にE（k11、P1（0））（k11・r1）^{e1}、E（k20，P2（1））（k20・r2）^{e2}、E（k31、P3（1））（k31・r3）^{e3}、E（k40、P4（0））（k40・r4）^{e4}を選んだことになる。

【0016】次に、第5の埋め込み処理として、ユーザは、選んだサーバ暗号化暗号鍵とすべてのサーバ暗号化乱数を自分の暗号鍵euで暗号化して、2重暗号化暗号鍵と2重暗号化乱数を生成してサーバに送る。

【0017】このとき、ユーザはすべてのサーバ暗号化乱数をつなぎ合わせた合成乱数等に対するハッシュ値に公開鍵暗号方式による署名を施してサーバに送る。これは、図4において、SigU（h（$r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}$））で表される。

【0018】次に、第6の埋め込み処理として、サーバは、署名をユーザの公開鍵を用いて検査した後、送られてきた2重暗号化暗号鍵と2重暗号化乱数の復号を行う。すなわち、暗号鍵enで暗号化されたデータに対してdn乗をしてmodをとる。

【0019】次に、復号した暗号化暗号鍵を、復号した暗号化乱数（ユーザ暗号化乱数）で割った結果（ユーザ暗号化暗号鍵）をユーザに送る。このとき、サーバは復号したSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と送られてきた署名を保存する。

【0020】図4では、これによって$k11^{eu}$、$k20^{eu}$、$k31^{eu}$、$k40^{eu}$、がユーザに送られ、$r1^{eu}$、$r2^{eu}$、$k31^{eu}$、$k40^{eu}$とSigU（h（$r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}$））がサーバに保存される。

【0021】次に、第7の埋め込み処理として、ユーザは、送られてきたユーザ暗号化暗号鍵を復号し、その復号された暗号鍵によって暗号化画像を復号し、分割された各ブロックを合成することによって電子透かし画像を得る。

【0022】図4では、送られたユーザ暗号化暗号鍵を復号する、すなわち、du乗してmodをとることによって暗号鍵k11、k20、k31、k40を得ることができる。この鍵は、上記第4の埋め込み処理で選択した暗号化画像の暗号鍵となっているので、この鍵で暗号化画像を復号することにより、P1（0）、P2（1）、P3（1）、P4（0）を得ることができる。

【0023】したがって、各ブロックを合成することによって、Sブロックにユーザ情報｛0，1｝をもち、Uブロックにはユーザによって選択された｛1，0｝のパターンをもつ電子透かし画像が得られる。

【0024】この手法では、ユーザがUブロックにどの数値が埋め込まれたブロックを選択したかをサーバは知ることができないので、サーバによる電子透かし画像の不正配布を行うことができない。

【0025】不正ユーザの特定は、サーバが不正画像からそのユーザのUブロックの数値、またはUブロックを暗号化した鍵を検証者に対して示すことによって認定される。不正画像が発見された場合、例えば、文献「〔BaBa．Iwamura，Zheng、Imai：'An Interactive Protocol for Image Fingerprinting'，SCIS98－10．2．E〕」では、検証処理は次のように行われる（図5参照）。

【0026】〔検証処理〕第1の検証処理として、サーバは、不正画像のSブロックからユーザ情報を取り出し、不正をしたと思われるユーザを特定する。次に、サーバは不正画像に基づいてUブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックを暗号化した暗号鍵を特定する。サーバは、特定したユーザ名、及び保存しているSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と署名、さらに上記第3の埋め込み処理で保存したすべてのサーバ暗号化乱数と、Sブロックに用いた乱数と、特定したUブロックの暗号鍵を検証者に渡して、以降の検証処理を依頼する。よって、図5ではサーバは検証者にユーザ名の他に「$r1^{eu}$、$r2^{eu}$、$k31^{eu}$、$k40^{eu}$、SigU（h（$r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}$））、$r1^{e1}$、$r2^{e2'}$、$r3^{e3'}$、r1、r2、k31、k40」を送る。

【0027】次に、第2の検証処理として、検証者は、提出されたサーバ暗号化乱数からハッシュ値を生成し、ユーザの公開鍵を用いて署名を検査し、一致するかどうか検査する。上記検査の結果が一致しない場合、そのサーバ暗号化乱数はそのユーザへの埋め込み処理に用いられたものではないので、ユーザは不正していないと認定される。

【0028】すなわち、$r1^{e1'}$、$r2^{e2'}$、$r3^{e3'}$、$r4^{e4'}$からハッシュ値h（$r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}$））を生成し、署名SigU

（ｈ（ｒ１$^{e1'}$‖ｒ２$^{e2'}$‖ｒ３$^{e3'}$‖ｒ４$^{e4'}$））をユーザの公開鍵で検査する。

【００２９】次に、第３の検証処理として、検証者は、上記第１の埋め込み処理で用いられたｐ（＝２ｑ＋１）を基にＮ組の異なる鍵を生成し、Ｓブロックの乱数とＵブロックの暗号鍵を暗号化し、順番を変えてユーザに送る。

【００３０】図５では、４組の暗号鍵（ｅ１”，ｄ１”）～（ｅ４”，ｄ４”）が生成され、Ｓブロックの乱数ｒ１、ｒ２と、Ｕブロックの暗号鍵ｋ３１、ｋ４０を「ｒ１^{e1}”、ｒ２^{e2}”、ｒ３^{e3}”、ｒ４^{e4}”」と暗号化し、順序を逆にしてユーザに送っている。

【００３１】次に、第４の検証処理として、ユーザは、送られてきたデータを埋め込み処理で用いた暗号鍵ｅｕによって暗号化してサーバに送る。図５では、「ｒ１^{e1}”^{eu}、ｒ２^{e2}”^{eu}、ｒ３^{e3}”^{eu}、ｒ４^{e4}”^{eu}」がサーバに送られる。ここで、Ｓブロックの乱数ｒ１、ｒ２とＵブロックの暗号鍵ｋ３１、ｋ４０は順番が変えられているので、ユーザはＳブロックとＵブロックに属するブロックを識別できない。

【００３２】次に、第５の検証処理として、サーバは、送られてきたデータを復号、すなわち、ｄｉ”乗してｍｏｄをとり、その結果を提出されたＳブロックのユーザ暗号化乱数とＵブロックのユーザ暗号化暗号鍵と比較する。

【００３３】Ｓブロックのユーザ暗号化乱数が一致しない場合、ユーザが埋め込み処理と異なる鍵で上記第４の検証処理を行ったことになり、ユーザの不正と認定される。また、Ｓブロックのユーザ暗号化乱数が一致し、Ｕブロックのユーザ暗号化暗号鍵が一致した場合もユーザの不正と認定される。

【００３４】それに対し、Ｓブロックのユーザ暗号化乱数が一致し、Ｕブロックのユーザ暗号化暗号鍵が一致しない場合のみユーザの不正と認定されない。よって、図５に示すように、Ｓブロックのユーザ暗号化乱数「ｒ１^{eu}、ｒ２^{eu}」とＵブロックのユーザ暗号化暗号鍵「ｋ３１^{eu}、ｋ４０^{eu}」とを比較する。

【００３５】

【発明が解決しようとする課題】上記の手法には、以下のような解決すべき問題点があった。第１の問題点として、Ｕブロックにおいて、暗号鍵と乱数の処理を逆にしても区別がつかないので、サーバはユーザに意図したＵブロックの鍵を使用させることができる問題があった。

【００３６】すなわち、図４において、Ｅ（ｋ３０，Ｐ３（０））（ｋ３０・ｒ３）^{e3}、Ｅ（ｋ３１，Ｐ３（１））（ｋ３１・ｒ３）^{e3}、ｒ３$^{e3'}$ の代わりに、Ｅ（ｋ３，Ｐ３（０））（ｋ３・ｒ３０）^{e3}、Ｅ（ｋ３，ｐ３（１））（ｋ３・ｒ３１）^{e3}、ｋ３$^{e3'}$ としても、以後、同様の処理が可能である（Ｐ４に関しても同様）。よって、サーバはユーザにＵブロックに関して意図した暗号鍵を使用させることができ、ユーザに罪を着せることが可能であった。

【００３７】また、第２の問題点として、上記第４の検証処理における暗号鍵ｅｕを用いた暗号化において、ユーザがＵブロックを暗号鍵ｅｕと異なる鍵で暗号化できれば、第５の検証処理においてＵブロックのユーザ暗号化暗号鍵が異なるためにユーザの不正と認定されない。

【００３８】しかし、第３の検証処理において、ユーザに送られる暗号化乱数と暗号化暗号鍵は並べ替えられているため、ユーザはＵブロックの暗号化暗号鍵を特定できないことが上述の文献における安全性の根拠になっている。

【００３９】しかし、不正画像の配布を行ったユーザが送られてきたデータの１つを暗号鍵ｅｕと異なる暗号鍵で暗号化して成功する確率はＮｕ／Ｎである。理論的には、上記Ｎを何万という非常に大きな値とし、上記Ｎｕを一桁台の値とすれば、ある程度の安全性は実現できるが、毎回すべてのユーザに対して画像を何万ピースにも分解して上記の埋め込み処理を行うことは、通信量や計算量等を考えると実用的及び効率的ではなかった。

【００４０】本発明は上述の問題点にかんがみ、ディジタルデータが不正に使用されるのを確実に防止できるようにするとともに、不正使用を防止するために行う通信量や計算量を減少できるようにすることを目的とする。

【００４１】

【課題を解決するための手段】本発明の電子透かし方式は、電子透かし情報の異なる複数の情報を生成する第１の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第２の処理と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第３の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第４の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の１つを選択する第５の処理を上記ユーザが行う電子透かし方式において、上記暗号鍵の一部にのみ乱数を乗じることを特徴としている。

【００４２】また、本発明の電子透かし方式の他の特徴とするところは、上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信することを特徴としている。

【００４３】また、本発明の電子透かし方式のその他の特徴とするところは、上記電子透かしの正当性を検証する処理を行うことを特徴としている。

【００４４】また、本発明の電子透かし方式のその他の特徴とするところは、上記電子透かしの正当性を検証する処理を繰り返して行うことを特徴としている。

【００４５】また、本発明の電子透かし方式のその他の特徴とするところは、電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処

理を用いて保証するようにした電子透かし方式において、上記ユーザの電子透かし情報を検査する処理を行うことを特徴としている。

【００４６】また、本発明の電子透かし方式のその他の特徴とするところは、上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する処理を行うことを特徴としている。

【００４７】また、本発明の電子透かし方式のその他の特徴とするところは、上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを用いることを特徴としている。

【００４８】また、本発明の電子情報配布システムは、電子透かし情報の異なる複数の情報を生成する第１の手段と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第２の手段と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第３の手段と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第４の手段とをサーバが有し、上記送信された複数の暗号化情報や、上記暗号化情報に対応する暗号化暗号鍵の１つを選択する第５の手段をユーザが有する電子情報配付システムにおいて、上記暗号鍵の一部にのみ乱数を乗じるようにする第６の手段をサーバに設けたことを特徴としている。

【００４９】また、本発明の電子情報配布システムの他の特徴とするところは、上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信する第７の手段を更に有することを特徴としている。

【００５０】また、本発明の電子情報配布システムのその他の特徴とするところは、上記電子透かしの正当性を検証する第８の手段をさらに有することを特徴としている。

【００５１】また、本発明の電子情報配布システムのその他の特徴とするところは、上記電子透かしの正当性を検証する処理を繰り返し行うようにしたことを特徴としている。

【００５２】また、本発明の電子情報配布システムのその他の特徴とするところは、電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子情報配付システムにおいて、上記ユーザの電子透かし情報を検査する検査手段を有することを特徴としている。

【００５３】また、本発明の電子情報配布システムのその他の特徴とするところは、上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する検査手段をさらに有することを特徴としている。

【００５４】また、本発明の電子情報配布システムのその他の特徴とするところは、上記暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報をヘッダ部に有する画像フォーマットを用いることを特徴としている。

【００５５】また、本発明の記憶媒体は、上記電子透かし方式方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴としている。

【００５６】また、本発明の記憶媒体の他の特徴とするところは、上記電子情報配布システムの各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴としている。

【００５７】

【作用】本発明は上記技術手段よりなるので、暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数が乗じられるので、暗号鍵と乱数の処理を逆にすることが防止され、サーバがユーザに意図した暗号鍵を使用させることができなくなる。

【００５８】また、本発明の他の特徴によれば、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透かし方式を実施する効率を大幅に向上させることができる。

【００５９】

【発明の実施の形態】以下、図１及び図６を参照して、上記第１の問題点を解決する第１の実施の形態を説明する。本実施の形態の手法は、Ｕブロックに対して乱数を用いず、Ｓブロックに対してのみ乱数を用いることによって、サーバがユーザに意図した暗号鍵を使用させることを防止しているものであり、プロトコルは以下のようになる。

【００６０】〔埋め込み処理〕先ず、図６のフローチャートのステップＳ６１に示したように、サーバが原画像をＮ個のブロックに分割し、各ブロックをＰｎ（ｎ＝１、…、Ｎ）とする。そして、原画像ＰｎをＮｓ個（Ｎｓ＜Ｎ）のＳブロックと、Ｎｕ個（Ｎｕ＝Ｎ－Ｎｓ）のＵブロックに分ける。

【００６１】図１では、原画像を４分割してブロックＰ１及びＰ２をＳブロックとし、Ｐ３及びＰ４をＵブロックとしている。また、サーバは暗号鍵ｋによってデータＰを暗号化する暗号化手段Ｅ（ｋ、Ｐ）を準備する（ユーザは、それに対応する復号手段を持つとする）。

【００６２】また、サーバとユーザは独立にｅ・ｄ＝１　ｍｏｄ　ｐ－１となる変数ｅと変数ｄを生成する。ただし、ｐ＝２ｑ＋１（ｑは素数）であり、サーバは以上のようなｅとｄをＮ＋Ｎｓ組生成し、（ｅｎ、ｄｎ）とおく（ユーザのｅとｄはｅｕ、ｄｕとおく）。

【００６３】次に、ステップＳ６２において、サーバはＳブロックにユーザ毎に定めたユーザ情報を埋め込む。次に、ステップＳ６３に進み、サーバはＵブロックの複製を2^b 個生成して、「０～2^b －１」の数値を埋め込む。以降、ブロックＰｎに数値ｉが埋め込まれた時、それをＰｎ（ｉ）と表現する。図１では、Ｓブロックであ

るＰ１、Ｐ２にユーザ情報として｛０，１｝が埋め込まれ、ｂ＝１としてＵブロックであるＰ３、Ｐ４の２個の複製に対して０～１の数値が埋め込まれている。

【００６４】次に、ステップＳ６４において、サーバはＳブロックのＰｎ（ｉ）の複製を2^b個生成し、各々異なる暗号鍵ｋｎｊ（ｊ＝０、…、2^b－１）で暗号化したＥ（ｋｎｊ、Ｐｎ（ｉ））と、暗号鍵ｋｎｊに乱数ｒｎをかけてｅｎで暗号化した$(knj \cdot rn)^{en}$をともにユーザに送る。

【００６５】さらに、サーバは、ステップＳ６５において、Ｎｕ・2^b個のＵブロックＰｎ（ｉ）を各々鍵ｋｎｉで暗号化したＥ（ｋｎｉ、Ｐｎ（ｉ））と、鍵ｋｎｉをｅｎで暗号化した$(kni)^{en}$をともにユーザに送る。また、Ｓブロックの乱数ｒｎをｅｎ’（ｎ’＝Ｎ＋ｎ）で暗号化したrn^{en}を保存し、かつユーザに送る。以後、Ｅ（ｋ、Ｐ）によって暗号化した画像を暗号化画像、暗号鍵をｅｕで暗号化したものをサーバ暗号化暗号鍵、またｅｎ’で暗号化した乱数をサーバ暗号化乱数と呼ぶ。このとき、暗号化画像やサーバ暗号化暗号鍵、サーバ暗号化乱数はその対応が正しければランダムに送ることができる。

【００６６】次に、ステップＳ６６において、ユーザは、送られてきた複数の暗号化画像とサーバ暗号化暗号鍵のペアの中から各ブロック毎に１つづつのペアを選ぶ。図１では、各ブロック毎にＥ（ｋ１１、Ｐ１（０））$(k11 \cdot r1)^{e1}$、Ｅ（ｋ２０、ｐ２（１））$(k20 \cdot r2)^{e2}$、Ｅ（ｋ３１、Ｐ３（１））$(k31)^{e3}$、Ｅ（ｋ４０、Ｐ４（０））$(k40)^{e4}$を選んだことになる。

【００６７】次に、ステップＳ６７において、ユーザは、選んだサーバ暗号化暗号鍵とすべてのサーバ暗号化乱数を自分の暗号鍵ｅｕで暗号化して、２重暗号化暗号鍵と２重暗号化乱数を生成してサーバに送る。このとき、ユーザはすべてのサーバ暗号化乱数をつなぎ合わせた合成乱数に対するハッシュ値に公開鍵暗号方式による署名を施してサーバに送る。これは、図１において、ＳｉｇＵ（ｈ（$r1^{e1'} \| r2^{e2'}$））で表される。

【００６８】次に、ステップＳ６８に示すように、サーバは、ユーザの公開鍵を用いて署名を検査した後、送られてきた２重暗号化暗号鍵と２重暗号化乱数の復号を行う。すなわち、ｅｎで暗号化されたデータに対してｄｎ乗してｍｏｄをとる。

【００６９】次に、ステップＳ６９において、サーバは復号した暗号化暗号鍵（ユーザ暗号化暗号鍵）を暗号化乱数（ユーザ暗号化乱数）で割り、その結果をユーザに送る。このとき、サーバは復号したＳブロックのユーザ暗号化乱数と、Ｕブロックのユーザ暗号化暗号鍵と、送られてきた署名を保存する。

【００７０】図１では、これによって「$k11^{eu}$、$k20^{eu}$、$k31^{eu}$、$k40^{eu}$」がユーザに送られ、「$r1^{eu}$、$r2^{eu}$、$k31^{eu}$、$k40^{eu}$」と、ＳｉｇＵ（ｈ（$r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}$））がサーバに保存される。

【００７１】次に、ステップＳ７０において、ユーザは送られてきたユーザ暗号化暗号鍵を復号し、その復号された暗号鍵によって暗号化画像を復号し、分割された各ブロックを合成することによって電子透かし画像を得る。図１では、送られたユーザ暗号化暗号鍵を復号する。すなわち、送られたユーザ暗号化暗号鍵をｄｕ乗してｍｏｄをとることによって暗号鍵ｋ１１、ｋ２０、ｋ３１、ｋ４０を得ることができる。

【００７２】この鍵は、ステップＳ６６で選択した暗号化画像の暗号鍵となっているので、この鍵で暗号化画像を復号することにより、Ｐ１（０）、Ｐ２（１）、Ｐ３（１）、Ｐ４（０）を得ることができる。

【００７３】よって、各ブロックを合成することによりＳブロックにユーザ情報｛０，１｝を持ち、ユーザによって選択された｛１，０｝のパターンをＵブロックに持つ電子透かし画像が得られる。

【００７４】上記のプロトコルに対応する検証処理は、従来技術で説明した第１の検証処理で検証者に送られる署名をＳｉｇＵ（ｈ（$r1^{e1'} \| r2^{e2''} \| r3^{e3'} \| r4^{e4''}$））からＳｉｇＵ（ｈ（$r1^{e1'} \| r2^{e2''}$））、サーバ暗号化乱数を「$r1^{e1'}$、$r2^{e2''}$、$r3^{e3'}$、$r4^{e4''}$」から「$r1^{e1'}$、$r2^{e2''}$」に変更すれば同様の処理によって実現できることは明らかである。

【００７５】これによって、暗号鍵と乱数の処理を逆にすることが防止され、サーバがユーザに意図した暗号鍵を使用させることができなくなる。また、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透かし方式を実施する効率を大幅に向上させることができる。

【００７６】また、安全性よりも計算量や通信量の削減や処理の簡単化を行う場合、すべての乱数ｒｎに関する処理を省略することもできる。この場合、上記ステップＳ６４において、Ｓブロックの複製を生成する必要はなく、１つの暗号鍵ｋｎによる暗号化Ｅ（ｋｎ、Ｐｎ（ｉ））と$(kn)^{en}$を作成すればよい。また、それ以降の乱数ｒｎに関するすべての処理を省略することができる。

【００７７】〔第２の実施の形態〕以下、上述した第２の問題点を解決するための実施の形態を、図２及び図７を参照して説明する。本実施の形態の手法は、画像分割数ＮとＵブロックの数Ｎｕに依存せず、検証処理を繰り返すことによって高い安全性を実現することができる。具体的な検証処理は以下のようになる。

【００７８】〔検証処理〕図７に示したように、サーバは、最初のステップＳ７１において、不正画像のＳブロックからユーザ情報を取り出し、不正を行ったと思われ

るユーザを推定する。次に、ステップＳ７２に進み、サーバは不正画像に基づいてＵブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックを暗号化した暗号鍵を特定する。

【００７９】次に、ステップＳ７３に進み、サーバは、特定したユーザ名、及び保存しているＳブロックのユーザ暗号化乱数とＵブロックのユーザ暗号化暗号鍵と署名、さらに上記埋め込み処理におけるステップＳ６５で保存したすべてのサーバ暗号化乱数と、Ｓブロックの乱数と、特定したＵブロックの暗号鍵を検証者に渡して検証を依頼する。

【００８０】よって、図２では、サーバは検証者にユーザ名の他に「$r1^{eu}$、$r2^{eu}$、$k31^{eu}$、$k40^{eu}$、$SigU(h(r1^{e1'} \| r2^{e2'} \| r3^{e3'} \| r4^{e4'}))$、$r1^{e1'}$、$r2^{e2'}$、$r3^{e3'}$、$r4^{e4'}$、ｒ１、ｒ２、ｋ３１、ｋ４０」を送る。

【００８１】検証者は、ステップＳ７４において、上記埋め込み処理におけるステップＳ６５で保存されたサーバ暗号化乱数からハッシュ値を生成し、ユーザの公開鍵を用いて署名を検査し、一致するかどうかを検査する。

【００８２】この検査の結果、署名が一致したか否かをステップＳ７５において判断する。そして、署名が一致しない場合には、そのサーバ暗号化乱数はそのユーザへの埋め込み処理に用いられたものではないので、ステップＳ７６に進み、ユーザは不正していないと認定する。

【００８３】一方、ステップＳ７５の検査結果が一致した場合には、ステップＳ７８に進み、検証者は、上記埋め込み処理で用いられたデータＰを基にＮ組の異なる鍵を生成し、Ｓブロックの乱数とＵブロックの暗号鍵を暗号化し、順番を変えてユーザに送る。

【００８４】図２では、４組の暗号鍵（$e1''$，$d1''$）～（$e4''$，$d4''$）が生成され、Ｓブロックの乱数ｒ１、ｒ２とＵブロックの暗号鍵ｋ３１、ｋ４０を、「$r1^{e1''}$、$r2^{e2''}$、$k31^{e3''}$、$k40^{e4''}$」と暗号化される。

【００８５】次に、ステップＳ７８に進み、ユーザは、送られてきたデータを埋め込み処理で用いた暗号鍵ｅｕによって暗号化してサーバに送る。図２では、「$r1^{e1''eu}$、$r2^{e2''eu}$、$k31^{e3''eu}$、$k40^{e4''eu}$」がサーバに送られる。ここで、Ｓブロックの乱数ｒ１、ｒ２とＵブロックの暗号鍵ｋ３１、ｋ４０は順番が変えられているので、ユーザはＳブロックとＵブロックに属すブロックを識別できない。

【００８６】次に、ステップＳ７９において乱数の比較処理を行うとともに、ステップＳ８０において鍵の比較処理を行う。これは、サーバが、送られてきたデータを復号、すなわち、ｄｉ”乗してｍｏｄをとり、その結果を保存されていたＳブロックのユーザ暗号化乱数とＵブロックのユーザ暗号化暗号鍵とを比較する。

【００８７】この比較の結果、Ｓブロックのユーザ暗号化乱数が一致しない場合はユーザが埋め込み処理と異なる鍵で上述した埋め込み処理を行ったことになるので、ステップＳ７９からステップＳ８１に進み、ユーザの不正と認定される。

【００８８】一方、Ｓブロックのユーザ暗号化乱数が一致し、Ｕブロックのユーザ暗号化暗号鍵が一致しない場合はユーザの不正と認定されない。また、Ｓブロックのユーザ暗号化乱数が一致し、Ｕブロックのユーザ暗号化暗号鍵が一致した場合もユーザの不正と認定される。よって、図２に示すように、Ｓブロックのユーザ暗号化乱数「$r1^{eu}$、$r2^{eu}$」とＵブロックのユーザ暗号化暗号鍵「$k31^{eu}$、$k40^{eu}$」を比較する。ただし、Ｓブロックのユーザ暗号化乱数が一致し、Ｕブロックのユーザ暗号化暗号鍵が一致しない場合はステップＳ８２に進んで所定の回数が終了したか否かを判断する。

【００８９】サーバは、所定の回数が終了したか、または納得が行けば処理を終了し、この場合はユーザの不正が認定されない。そうでない場合、上述した検証処理を繰り返す。以上の検証処理において、不正を行ったユーザが１つのブロックを異なる暗号鍵で暗号化したとすると、Ｎｕ／Ｎの確率で成功する（検証者によってユーザの不正と認定されない）。

【００９０】上述した検証処理において、上記ステップＳ７７～ステップＳ８２の処理をｋ回繰り返すとすると、不正を行ったユーザは常に同じブロックを異なる暗号鍵で暗号化する必要があるが、ステップＳ７７において、サーバが送るデータは順番が毎回異なるので、ユーザは前回異なる暗号鍵で暗号化したブロックを特定できない。

【００９１】よって、本実施の形態の検証処理では、不正を行ったユーザは$(Nu/N)^k$の確率でしか成功せず、ｋの値を大きくすることによって画像の分割に依存せず、検証処理の安全性を高めることができる。

【００９２】また、第１の実施の形態の埋め込み処理に本実施の形態の検証処理を適用する場合、本実施の形態の検証処理で検証者に送られる署名を$SigUj(h(r1^{e1'} \| r2^{e2''} \| r3^{e3'} \| r4^{e4''})$から、$SigU(h(r1^{e1'} \| r^{e2''})$、サーバ暗号化乱数を「$r1^{e1'}$、$r2^{e2''}$、$r3^{e3'}$、$r4^{e4''}$」から，「$r1^{e1'}$、$r2^{e2''}$」に変更すれば、同様の処理によって安全性の高い検証処理を実現することができる。

【００９３】〔第３の実施の形態〕以下、上記第２の問題点を解決する実施の形態を図３及び図８を参照して詳細に説明する。この手法は、上記第２の実施の形態で示した検証処理のように、暗号的手法を用いずに直接画像を検査することによって検証処理を軽減することができる。

【００９４】具体的な手順は、以下のようになる。ただし、埋め込み処理の前にサーバはユーザから画像購入に関する契約情報を入手しているとし、検証者は電子透か

し情報の抽出法を知っているとする。

【００９５】〔検証処理〕図８のステップＳ８１に示したように、サーバは、不正画像のＳブロックからユーザ情報を取り出し、不正をしたと思われるユーザを推定する。次に、ステップＳ８２に進み、サーバは上記推定した不正画像に基づいて、Ｕブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックに埋め込んだ数値を特定する。

【００９６】次に、ステップＳ８３に進み、サーバは、上記特定したユーザ名、及びそのユーザからの契約情報と、Ｓブロックに埋め込まれた数値と、Ｕブロックに埋め込まれた数値を検証者に渡して検証を依頼する。

【００９７】よって、図３ではサーバは検証者にユーザ名のほかに、ユーザからの契約情報（ＳｉｇＵ（Ｃ）と表し、Ｃはユーザ名などを特定したユーザからの購入希望文書であり、ＳｉｇＵ（）はそのユーザにより署名がなされていることを表す）と、各ブロックから特定した数値（０、１、１、０）を送っている。

【００９８】次に、ステップＳ８４に進み、検証者は、契約情報を確認する。検証者は購入した画像をユーザから提出させる（図３参照）。

【００９９】次に、ステップＳ８５において、検証者は、ユーザから提出された画像の各ブロックから埋め込まれた数値を抽出する。そして、次のステップＳ８６において、上記抽出した数値とサーバから示された数値とが一致するかを各ブロック毎に比較する。

【０１００】この比較の結果、ユーザ画像から抽出された数値とサーバから提出された数値とが一致した場合にはユーザの不正と認定され、一致しない場合ユーザの不正と認定されない。

【０１０１】本実施の形態は、従来の方式の埋め込み処理、及び第１、第２の実施の形態の埋め込み処理に対して適用できることは明らかである。さらに、本実施の形態により検証処理を行う場合、埋め込み処理におけるサーバによる暗号化乱数や暗号化暗号鍵の保存や、ユーザによる暗号化乱数のハッシュ値に対する署名の処理を省略できることも明らかである。

【０１０２】また、検証局は電子透かし情報を抽出できるので、電子透かし情報抽出のための秘密鍵を知り、信頼できる機関である必要があるので、鍵供託システムまたは鍵復元システムにおける鍵管理局とすることも考えられる。

【０１０３】〔その他の実施の形態〕透かし情報の埋め込みは公知の埋め込み手法によって実現できるが、例えば電子透かしを埋め込み方法の例としては、離散コサイン変換を利用するものとしてＮＴＴの方式（中村、小川、高鳴、”ディジタル画像の著作権保護のための周波数領域における電子透かし方式”ＳＣＩＳ－９７－２６Ａ，１９９７年１月）の他に、離散フーリエ変換を利用するものとして防衛大の方式（大西、岡、松井、”ＰＮ系列による画像への透かし署名法”ＳＣＩＳ－９７２６Ｂ、１９９７年１月）や、離散ウェーブレット変換を利用するものとして三菱、九大の方式（石塚、坂井、櫻井、”ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”、ＳＣＩＳ’１９９７年１月）などが挙げられる。

【０１０４】また、暗号処理Ｅ（ｋ，Ｐ）は、種々の暗号方式によって実現できるが、例えば、ＤＥＳやＦＥＡＬ等のような共通鍵暗号方式によって容易に実現することができる。

【０１０５】また、上述の実施の形態の画像分割は、図１～図３に示したような平面的な分割だけでなく、多値画像における各位に対応するビットプレーンやＲＧＢのような色毎の分割や、合成すれば元の画像に電子透かしが埋め込まれた画像になる分割手法を全て含む。また、原画像となるものは、静止画像に限定されず、動画像や音声などすべてのディジタル情報を含むことができる。

【０１０６】また、上述の実施の形態では不正画像の検出はサーバが行っているが、不正画像の発見者はサーバに限定されず、特定の検査機関や電子透かしの抽出法を知る他者が行うことが可能である。

【０１０７】また、サーバからの暗号化画像とサーバ暗号化暗号鍵、サーバ暗号化乱数等はネットワークやＣＤ－ＲＯＭ等によって広く配布されていてもよい。また、暗号化画像に対応するサーバ暗号化暗号鍵、サーバ暗号化乱数にサーバが署名を施し、その対応を保証することも可能である。

【０１０８】また、埋め込み処理を行う前にユーザからの画像データを要求する契約情報がサーバによせられることが考えられる。このとき、契約情報がユーザの公開鍵暗号方式を用いた署名によって実現されることもある。

【０１０９】また、その署名を検査する公開鍵が認証局によって保証されていることも考えられる。この場合、その公開鍵とユーザとの関係が認証局によって秘密に保たれれば、ユーザの匿名性を実現することもできる。

【０１１０】また、サーバとユーザとの間に画像販売の代理を行う代理店があるシステムに用いることも可能である。このとき、埋め込み処理のサーバ暗号化乱数やサーバ暗号化暗号鍵の生成をサーバと代理店とで分担して行ったりすることもできる。

【０１１１】〔第４の実施の形態〕本発明に示したサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等は、任意の画像フォーマットで格納することができる。特に、一般的な画像フォーマットでは、送付される電子透かし画像データまたは暗号化画像を画像データ部に格納し、その電子透かしに対するサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等を含む種々の情報をヘッダ部に格納することができる。

【０１１２】一方、下記に示すＦｌａｓｈＰｉｘＴＭフ

ァイルフォーマットでは、上記のようなサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、サーバまたはユーザによる暗号化暗号鍵や暗号化乱数等は属性情報としてプロパティセットの中に格納しておくこともできる。

【0113】以下、説明するＦｌａｓｈＰｉｘTM（ＦｌａｓｈＰｉｘは米国Ｅａｓｔｍａｎ　Ｋｏｄａｋ社の登録商標）ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データをさらに構造化してファイル内に格納する。

【0114】上記構造化した画像ファイル内の各プロパティやデータにはＭＳ－ＤＯＳのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。画像データや画像属性情報はストリーム部分に格納される。

【0115】画像データは、異なる解像度で階層化されており、それぞれの解像度の画像をＳｕｂｉｍａｇｅと呼び、Ｒｅｓｏｌｕｔｉｏｎ　０、１…ｎで示す。各解像度画像に対して、その画像を読み出すために必要な情報がＳｕｂｉｍａｇｅ　ｈｅａｄｅｒに格納され、また画像データがＳｕｂｉｍａｇｅ　ｄａｔａに格納される。

【0116】ここで、プロパティセットとは、属性情報をその使用目的、内容に応じて分類して定義したもので、Ｓｕｍｍａｒｙ　Ｉｎｆｏ．Ｐｒｏｐｅｒｔｙ　Ｓｅｔ，Ｉｍａｇｅ　Ｉｎｆｏ　Ｐｒｏｐｅｒｔｙ　Ｓｅｔ，Ｉｍａｇｅ　Ｃｏｎｔｅｎｔ　Ｐｒｏｐｅｒｔｙ　Ｓｅｔ、Ｅｘｔｅｎｓｉｏｎ　ｌｉｓｔ　ｐｒｏｐｅｒｔｙ　Ｓｅｔがある。

【0117】Ｓｕｍｍａｒｙ　Ｉｎｆｏ．Ｐｒｏｐｅｒｔｙ　Ｓｅｔは、ＦｌａｓｈＰｉｘ特有のものではなく、Ｍｉｃｒｏｓｏｆｔ社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。

【0118】Ｉｍａｇｅ　Ｃｏｎｔｅｎｔｓ　Ｐｒｏｐｅｒｔｙ　Ｓｅｔは，画像データの格納方法を記述する属性である。この属性には、画像データの階層数、最大解像度の画像の幅及び高さや、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはＪＰＥＧ圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義を記述する。

【0119】Ｉｍａｇｅ　Ｉｎｆｏ．Ｐｒｏｐｅｒｔｙ　Ｓｅｔは、画像を使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの情報を格納する。

【0120】Ｅｘｔｅｎｓｉｏｎ　ｌｉｓｔ　ｐｒｏｐｅｒｔｙ　Ｓｅｔは、ＦｌａｓｈＰｉｘの基本仕様には含まれない下記（イ）～（リ）の情報を追加する際に使用する領域である。

（イ）ディジタルデータの取り込み方法／あるいは生成方法に関する情報（Ｆｉｌｅ　Ｓｏｕｒｃｅ）、（ロ）著作権に関する情報（Ｉｎｔｅｌｌｅｃｔｕａｌ　ｐｒｏｐｅｒｔｙ）（ハ）画像の内容（画像中の人物、場所など）に関する情報（Ｃｏｎｔｅｎｔｄｅｓｃｒｉｐｔｉｏｎ）、（ニ）撮影に使われたカメラに関する情報（Ｃａｍｅｒａ　ｉｎｆｏｒｍａｔｉｏｎ）、（ホ）撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無など）の情報（Ｐｅｒ　Ｐｉｃｔｕｒｅ　ｃａｍｅｒａｓｅｔｔｉｎｇｓ）、（ヘ）ディジタルカメラ特有解像度やモザイクフィルタに関する情報（Ｄｉｇｉｔａｌ　ｃａｍｅｒａ　ｃｈａｒａｃｔｅｒｉｚａｔｉｏｎ）、（ト）フィルムのメーカ名、製品名、種類（ネガ／ポジ、カラー／白黒）などの情報（Ｆｉｌｍ　ｄｅｓｃｒｉｐｔｉｏｎ）、（チ）オリジナルが書物や印刷物である場合の種類やサイズに関する情報（Ｏｒｉｇｉｎａｌ　ｄｏｃｕｍｅｎｔ　ｓｃａｎ　ｄｅｓｃｒｉｐｔｉｏｎ）、（リ）スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報（Ｓｃａｎ　ｄｅｖｉｃｅ）、

【0121】なお、ＦｌａｓｈＰｉｘにおいて、ＦｌａｓｈＰｉｘ　Ｉｍａｇｅ　ＶｉｅｗＯｂｊｅｃｔは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する、画像ファイルである。

【0122】上記ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応させるために記憶しておく処理係数のセットである。

【0123】Ｓｏｕｒｃｅ／Ｒｅｓｕｌｔ　ＦｌａｓｈＰｉｘ　Ｉｍａｇｅ　Ｏｂｊｅｃｔは、ＦｌａｓｈＰｉｘ画像データの実体であり、Ｓｏｕｒｃｅ　ＦｌａｓｈＰｉｘ　Ｉｍａｇｅ　Ｏｂｊｅｃｔは必須であり、Ｒｅｓｕｌｔ　ＦｌａｓｈＰｉｘＩｍａｇｅ　Ｏｂｊｅｃｔはオプションである。

【0124】Ｓｏｕｒｃｅ　ＦｌａｓｈＰｉｘ　Ｉｎａｇｅ　Ｏｂｊｅｃｔは、オリジナルの画像データを、Ｒｅｓｕｌｔ　ＦｌａｓｈＰｉｘ　Ｉｍａｇｅ　Ｏｂｊｅｃｔはビューイングパラメータを使って画像処理した結果の画像を格納する。

【0125】Ｓｏｕｒｃｅ／Ｒｅｓｕｌｔ　ｄｅｓｃ．Ｐｒｏｐｅｒｔｙ　ｓｅｔは上記画像データの識別のためのプロパティセットであり、画像ＩＤ、変更禁止のプロパティセット、最終更新日時等を格納する。

【0126】Ｔｒａｎｓｆｏｒｍ　ｐｒｏｐｅｒｔｙ　ｓｅｔは回転、拡大／縮小、移動のためのＡｆｆｉｎｅ変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【0127】また、上記実施の形態におけるハッシュ値、認証局、公開鍵暗号方式、共通鍵暗号方式を、以下

にまとめて説明する。すなわち、ハッシュ値とは、ハッシュ関数hの出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは異なるｘ１．ｘ２に対してｈ（ｘ１）＝ｈ（ｘ２）となることである。

【０１２８】また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは任意のビット長のビット列をある長さのビット列に変換する関数であり、ｈ（ｘ１）＝ｈ（ｘ２）を満たすｘ１、ｘ２を容易に見出せないものである。

【０１２９】このとき、任意のｙからｙ＝ｈ（ｘ）を満たすｘを容易に見出せないので、必然的にハッシュ関数は一方向性関数となる。ハッシュ関数の具体例としては、ＭＤ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ）５や、ＳＨＡ（Ｓｅｃｕｒｅ　ＨａｓｈＡｌｇｏｒｉｔｈｍ）等が知られている。

【０１３０】〔認証局〕公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を認証局と言う。すなわち、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成して発行する。

【０１３１】例えば、あるユーザから自分の証明書付き公開鍵を送られたユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織としてＶｅｒｉＳｉｇｎや、ＣｙｂｅｒＴｒｕｓｔという企業がよく知られている。

【０１３２】〔公開鍵暗号方式〕公開鍵暗号方式は、暗号鍵と復号鍵とが異なり、暗号鍵を公開にし、復号鍵を秘密に保持するようにしている暗号方式である。

【０１３３】代表例として、ＲＳＡ暗号やＥｌＧａｍａｌ暗号等が知られている。以下の（１）～（３）ような特徴をもち、秘密通信や認証通信等を実現することができる。

（１）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるために暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

【０１３４】（２）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

【０１３５】（３）送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【０１３６】〔鍵供託システムまたは鍵復元システム〕鍵供託システムまたは鍵復元システムとは、暗号鍵を信頼できる第３者に預けて、犯罪や鍵紛失等が起こった場合に、その第３者から暗号鍵の入手が可能になっているシステムをいう。

【０１３７】（本発明の他の実施形態）本発明は複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【０１３８】また、上述した実施形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【０１３９】また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１４０】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【０１４１】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【０１４２】

【発明の効果】上述の説明から明らかなように、本発明によれば、暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数が乗じられるので、暗号鍵と乱数の処理を逆にすることを防止することができる。これにより、サーバがユーザに意図した暗号鍵を使用させないようにすることができ、サーバが利用者情報を勝手に埋め込みそのコピーを不正に配布することを防止することができる。

【０１４３】また、本発明の他の特徴によれば、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透か

し方式を実施する効率を大幅に向上させることができ、ディジタルデータの不正配布に関して安全で高効率なシステムを実現することができる。

【図面の簡単な説明】

【図1】第1の実施の形態に示した埋め込み処理を説明するための図である。

【図2】第2の実施の形態に示した検証処理を説明するための図である。

【図3】第3の実施の形態に示した検証処理を説明するための図である。

【図4】従来の埋め込み処理を説明するための図である。

【図5】従来の検証処理を説明するための図である。

【図6】第1の実施の形態に示した埋め込み処理の手順を説明するためのフローチャートである。

【図7】第2の実施の形態に示した検証処理の手順を説明するためのフローチャートである。

【図8】第3の実施の形態に示した検証処理の手順を説明するためのフローチャートである。

【符号の説明】

P1，P2，P3，P4　ブロック画像

k　暗号鍵

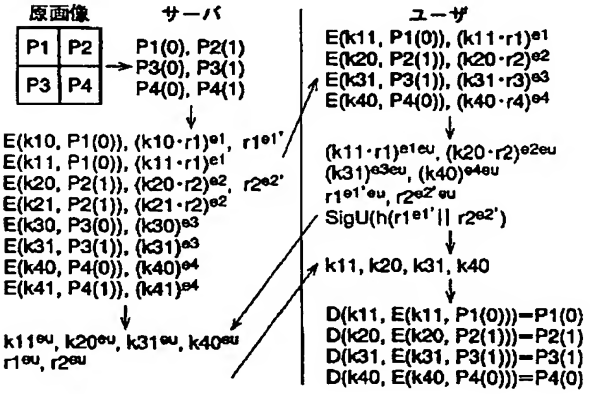
E（k，P）　暗号化手段

e　サーバ暗号鍵

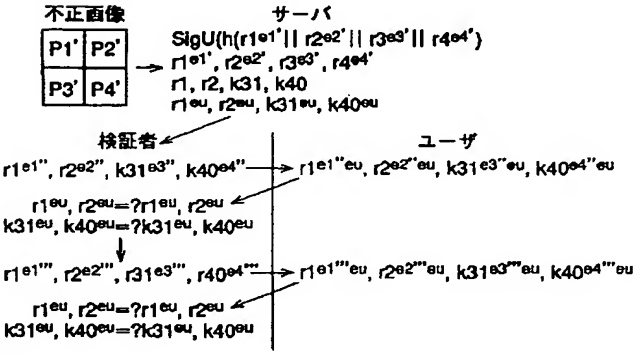
eu　ユーザ暗号鍵

SigU　署名

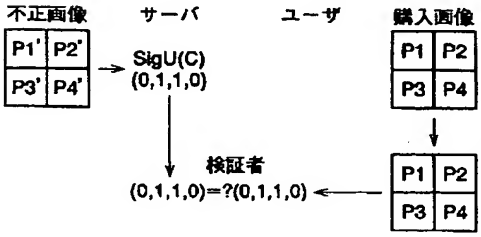
【図1】



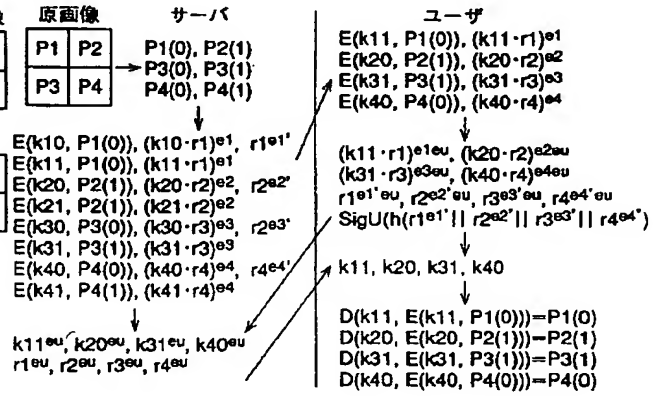
【図2】



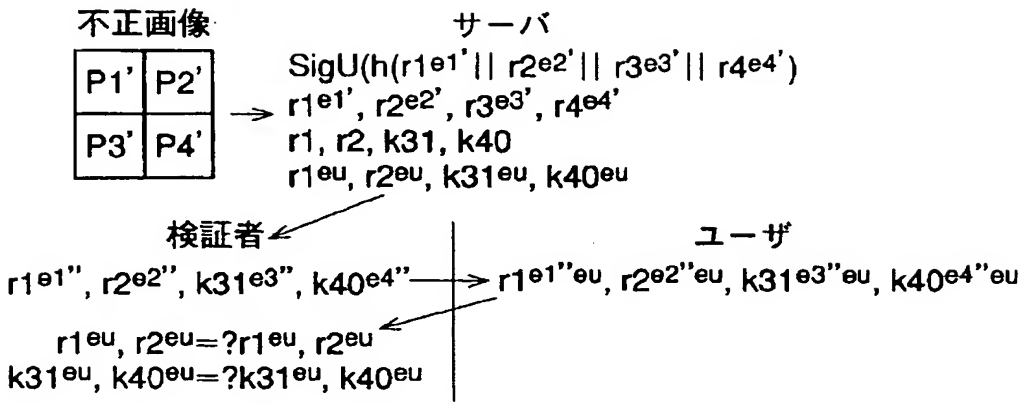
【図3】



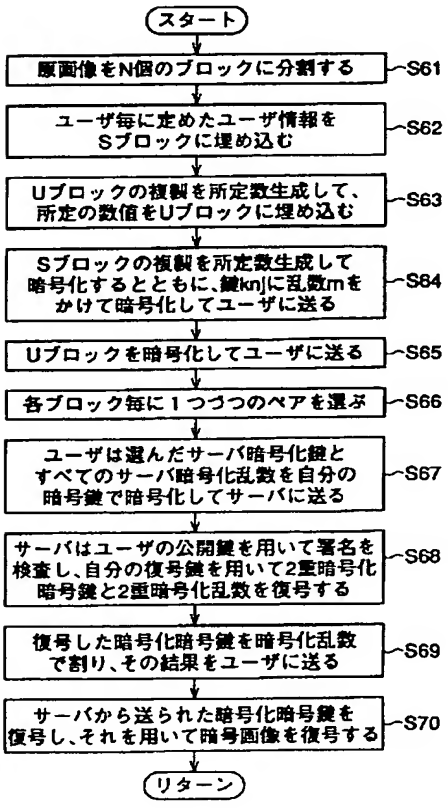
【図4】



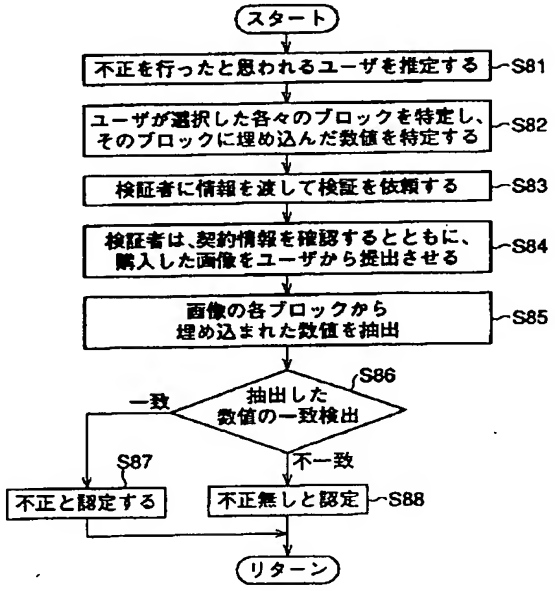
【図５】


不正画像
P1'
P2'
P3'
P4'
サーバ
SigU(h(r1e1'|| r2e2'|| r3e3'|| r4e4')
r1e1', r2e2', r3e3', r4e4'
r1, r2, k31, k40
r1eu, r2eu, k31eu, k40eu
検証者
ユーザ
r1e1'', r2e2'', k31e3'', k40e4''
r1e1''eu, r2e2''eu, k31e3''eu, k40e4''eu
r1eu, r2eu=?r1eu, r2eu
k31eu, k40eu=?k31eu, k40eu

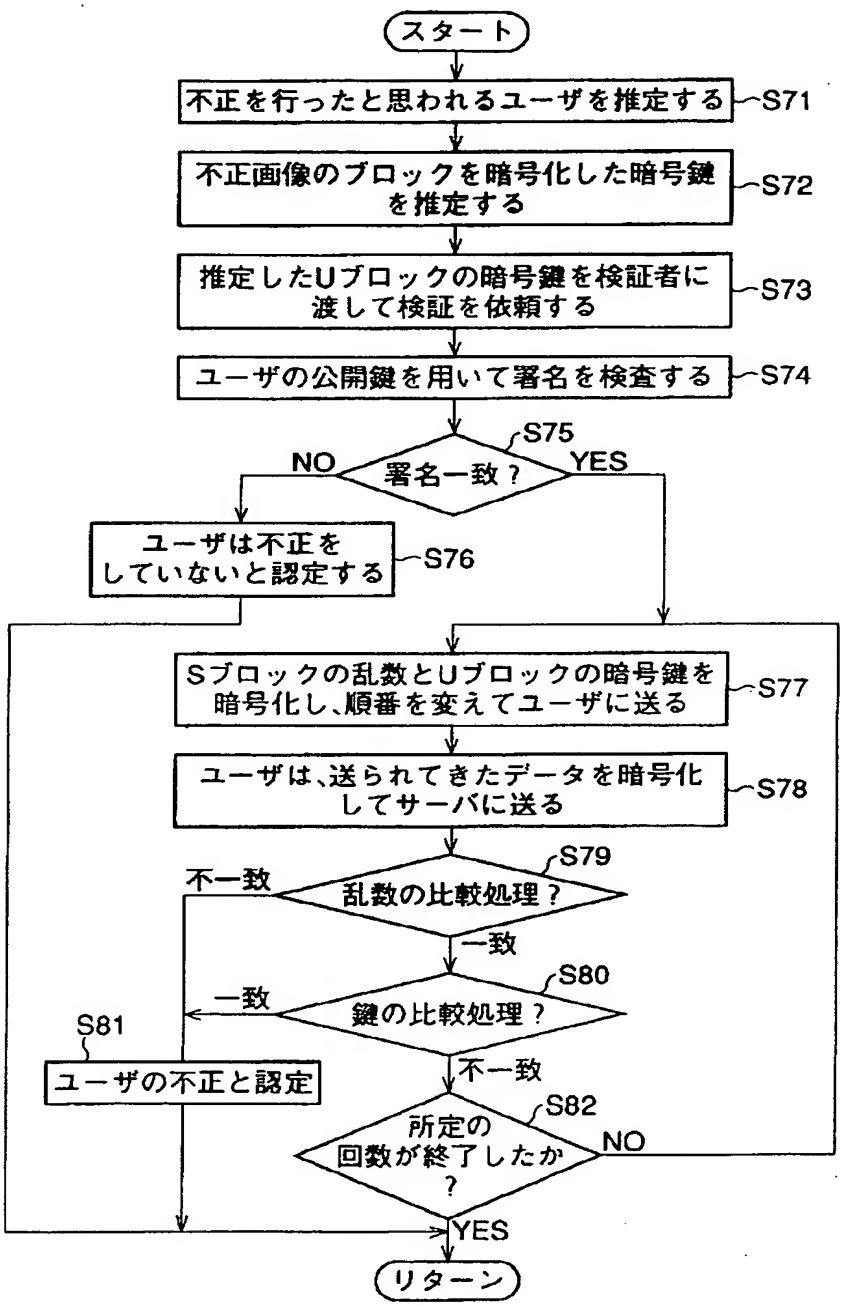
【図６】


スタート
原画像をN個のブロックに分割する
S61
ユーザ毎に定めたユーザ情報を
Sブロックに埋め込む
S62
Uブロックの複製を所定数生成して、
所定の数値をUブロックに埋め込む
S63
Sブロックの複製を所定数生成して
暗号化するとともに、鍵kn|に乱数mを
かけて暗号化してユーザに送る
S64
Uブロックを暗号化してユーザに送る
S65
各ブロック毎に１つづつのペアを選ぶ
S66
ユーザは選んだサーバ暗号化鍵と
すべてのサーバ暗号化乱数を自分の
暗号鍵で暗号化してサーバに送る
S67
サーバはユーザの公開鍵を用いて署名を
検査し、自分の復号鍵を用いて2重暗号化
暗号鍵と2重暗号化乱数を復号する
S68
復号した暗号化暗号鍵を暗号化乱数
で割り、その結果をユーザに送る
S69
サーバから送られた暗号化暗号鍵を
復号し、それを用いて暗号画像を復号する
S70
リターン

【図８】


スタート
不正を行ったと思われるユーザを推定する
S81
ユーザが選択した各々のブロックを特定し、
そのブロックに埋め込んだ数値を特定する
S82
検証者に情報を渡して検証を依頼する
S83
検証者は、契約情報を確認するとともに、
購入した画像をユーザから提出させる
S84
画像の各ブロックから
埋め込まれた数値を抽出
S85
S86
抽出した
数値の一致検出
一致
不一致
S87
不正と認定する
不正無しと認定
S88
リターン

【図7】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04N	5/91		H04N	5/91	P
	7/08			7/08	Z

7/081